IOT Security - 2016

Who We Are:

A 13-member team providing security policy and some aspects of security operations. Our team works with the operational teams of IOT and the agencies to mitigate risks to confidential state data.

Our Mission:

To provide information security and related services that preserve the value of state-held assets while supporting the State's business objectives.

Department: 493003

Managers

Tad Stahl, CISO; Nick Sturgeon, SOC Manager

When We Were Formed:

The IOT Security team was formed in October 2005.

What We Do:

IOT Security sets information security policy for the Executive Branch of state government and then works with agencies to protect confidential citizen data by working toward compliance with those policies. IOT Security also operates a number of enterprise-wide protective tools and processes. IOT Security also designs and implements the State's disaster recovery plan.

Our Products:

1175	Security - Baseline
1180	Security - Confidential
1137P	Disaster Recovery - Physical Server
1137V	Disaster Recovery - Virtual Server

Our Tools:

Antivirus/Malware
FireEye NX – Network malware detections (workstation specific)
Intel (McAfee) ePO, HIPS, ATD, TIE, SiteAdvisor
MS-ISAC (managed 3rd party sensor)

Internet Traffic Management
Citrix NetScaler
Intel (McAfee) Web Gateways
Intel SiteAdvisor – browser plugin
MS-ISAC (managed 3rd party sensor)

Intrusion Detection/Prevention
Cisco IPS
Citrix NetScaler
MS-ISAC (managed 3rd party sensor)

Vulnerability Scanning
Nexpose Rapid 7

Email Protection
FireEye EX
Intel (McAfee) Mail Gateway
Sophos

Asset Management/Protection
Absolute – track stolen equipment
Intel SIR
Mobile Iron (smart phones/tablets)

Logging
Intel ESM SIEM

Database
Intel Database Access Management

Privilege Management
Avecto
Microsoft ATA
Microsoft Azure (two-factor)

Our Metrics:

IOT Security tracks a number of metrics for its protective tools. This year we will begin tracking agency compliance with the NIST framework.

Our Customers:

All Executive Branch agencies.

Our Budget: $10M

Major Accomplishments - 2015:

- Established security rates (baseline, confidential systems) allowing the state to pursue protections against the following threats (and others):
    - Hackers
    - Social engineering, malware
    - Malicious insiders
    - Human error
- Implemented protective tools
    - Procured FireEye, implemented email and network protections
    - Procured Archer, implemented SecOps module
    - Implemented McAfee ATD, TIE and SolidCore
- Started the Security Operations Center (SOC)
- Refreshed and completed the acceptance process for the State's acceptable use agreement (IRUA)

Current Projects:

- Implementation of Microsoft ATA
- Implementation of asset management, Archer
- Implementation of NIST compliance, Archer
- SOC security awareness coordination, creation, distribution
- Upgrading vulnerability management capability
- Evaluating file management tools
- Monitoring operational teams security projects
- Rewriting policy following the NIST framework